



2600 is published by 2600 Enterprises, Inc., an ecclesiastical organization.
 Subscription rates: \$39—1 year, \$5—6 months, \$1 per back issue. Overseas: \$17.50—1 year.
 Lifetime subscription: \$200. Corporate sponsorship: \$2500.

Write to: 2600, Box 752, Middle Island, NY 11953-0152. Dial: 516/7512600. BBS: 201/666431. ISSN: 0749-3851.

VOLUME TWO, NUMBER THREE

NAZI BBS A CHALLENGE TO HACKERS

One of our correspondents made an interesting discovery last month. She found the telephone number for one of the computer bulletin board systems operated by American Nazis. With this number she was able to log on and get the information that the media has lately been all huzzeyed about. Now we are prepared to talk intelligently on the matter.

For one thing, this bulletin board is an Apple running Network software. There are only about two dozen messages posted on it. Only people who pay \$5 can post messages or use electronic mail functions. The system is not used very often judging from the frequency of the messages. The people behind it seem to have no interest in changing anything in the software or doing anything imaginative with it. (Example: on most Apple bulletin boards, the "B" command gets you a list of other bulletin board systems. At the end of the list, the program prints, "When calling other systems, be sure to tell them about [name of board]. This message can easily be changed. The Nazis use the "B" command also, except they use it to list addresses of "patriot" groups. Even though the list is not a list of bulletin boards, you still get the "When calling other systems" message at the end of it.)

There seems to be little or no attendance by any sysop based on zero chat availability and no replies to all kinds of feedback. "G" files exist (standards on Apple boards, usually used for storing large articles), however one of them requires Level 7 access. Or at least, that's what it says. The file in question is a list of race traitors, their addresses, etc. We are convinced that no such file exists, at least not there. When requesting this file, you are told: "Here is a list of race traitors. Level 7 access required." This doesn't seem right. Either you're allowed

to read the file or not. In this case, you're allowed to read part of the file and then suddenly you aren't. It's almost as if the file simply contains the above statement and nothing else. Unfortunately, the media never picked up on that.

Our point here is simply this: you computer hackers and phone phreaks that are reading this have the ability to uncover and analyze circumstances in ways that most people can't. Some of you have the ability to recognize touch tones by ear. A few can tell where their calls are going by the sounds they hear. And still others are able to get into more than a few major systems and find the interesting stuff almost immediately. There is a very definite need in this world for such intelligence. Every authority figure in existence would like to get a piece of your abilities but very few are deserving of them. Besides, who really enjoys selling out?

Think of all the events going on in the world today. When all phone lines to Poland are cut off, use your tricks to route through Belgrade. Then let the press know that you can get through if they care. Track down interesting people in South Africa, El Salvador, the Soviet Union—especially in times of crisis. There's no reason why you cannot attain the same respectability that a ham radio operator has when things get desperate. We can all still have lots of fun, and at the same time move some mountains.

The Nazis are a start. If hackers can uncover a thing or two that nobody else knows about, we'll be on the road to finally being appreciated. Let us know what you find. But be careful out there.

The numbers for the Nazi boards are 2142631106 and 9193239888. If you would like a full printout of all of the messages contained on these boards, send \$5 to 2600, Box 752, Middle Island, NY 11953-0752.

are you a phreak???

by Bob Gamma

From the mere jokeline caller to the telecommunications wizard, one can find phone folks at various levels of the phone kingdom. These are not definitive boundaries, for even the most knowledgeable phreaks occasionally revert to primitive tactics:

The Dippy Dialer. The person who got a Zygote Dial-A-Joke number from their little sister and is forever trying to get through the busy signal which other Dippy Dialers have caused. Not to be totally ignored, since it is this person who keeps the entertainment lines in business. Even though they do not know the difference between the prefix and the area code, they are the only people that find the jokes to be humorous. This brand of lowlife makes prank phone calls (sample: "Is your refrigerator running? Then you better go catch it!") and has been known to run up his parents' phone bill on long distance calls which he thought were local.

Conference Brat/Loop Idiot. Has an interminable list of test numbers, WATS goodies, other phreaks' private numbers, and searches endlessly for working loops. Known to (abuse the Alliance Teleconferencing mechanism. Typified by playing the "info exchange game" and dreams of the day that he will have his own phone line. This creature also calls the phone phun lines, but overstacks SPC and MCI trunks. Also enjoys leaving lengthy disconnects on other people's answering machines.

Amateur Phone Phreak. Has 16 illegal extensions with touch tone and homemade hold buttons. Collects telephone directories of cities he can't spell or find on the map. Also accumulates Bell paraphernalia like pay phone instruction cards and stationery from the security division for scaring his friends. These mischievous types wire coin phones to always

refund, harass telco installers, and raid the central office trash containers for research material. Has the cheapest measured service line, but with all the custom calling features. Collects coin phone refund checks from the BOC's and independent telcos, including 3rd rate companies like GTE. Fantasizes of working for Ma Bell someday.

Phone Phreak Extraordinaire. Has a key system for his 4 phone lines, of which he only answers one. Has a pager, but still is impossible to track down. Charter subscriber to 2600. He knows every free call there is and talks to the East Coast phreaks not so much for phreaking but to laugh at their accents. Dabbles with computer systems, but has no respect for its security. Can answer any question about the telephone except why he likes it. Has at least one 3-slot pay phone proudly displayed on his wall, and is the only person with an appreciation of independent telcos, step-by-step switching, and divestiture.

Phone Phreak Emeritus. Retired from the service after getting busted 3 times: For Sprinting across the country; For violating probation by blue boxing (telco security confiscated his blue box); And finally for hacking COSMOS. Has no phone line at all, as he is paranoid that the temptation would be too great. Tries new hobbies such as needlepoint and stamp collecting in order to lessen phone phreak withdrawal pains. Meticulously avoids breaking any laws: drives 55 mph on highways. This nasty streak of morality could probably be cured by giving him a butt phone and locking him in a feeder closet which contains 200 unrestricted dial tones.

Where do you fit in? Tell your friends where they belong. Then change your phone number, quickly!

HOW TO GET INTO A C.O.

by The Kid & Co.

Having spent a lot of time crashing outside the CO, I decided it was time to see what was inside. Well, the first idea that came to mind was to try and make my own informal tour. This was impossible due to the magnetic lock on the door. So my next thought was why not try to arrange a tour legitimately? Who would expect a phreak to try that??

A call to the business office started me on my way. They in turn gave me the phone number of the Public Relations people, who told me to send a letter to a primary switching office in my area. I anxiously waited for several weeks. Then one day I received an urgent phone call from the telco while I was out. Thinking it was Bell Security, I became nervous. I called back but the person who called was out. So I had to wait. Sure enough he called back. I was very relieved when he informed me that he was calling about the tour I had requested. I was also surprised to find that he sounded like a reasonable human being. We worked out some details and set up a date for the tour. I now had to select the group to go with me and prepare some questions.

I could bring up to 10 people on the tour. My obvious first choice was my friend, The Shadow. The real problem was who else could I bring? I did not want to take a chance on someone saying too much and thus creating a problem. So I chose several others, sticking to people who were just interested in the tour because they wanted to know what the CO was, but weren't smart enough to ask embarrassing questions.

The Shadow and I spent several hours preparing questions to get the maximum benefit from the tour. We found that those few hours we spent preparing ourselves were well worth the time. We started with simple questions to which we already knew the answers. These would lead to the more complex and specific questions, without revealing our true identities as telecommunications hobbyists.

After weeks of waiting, the day of the CO tour arrived. We were ready! Notebooks in hand, ready to record the commentary, we drove the familiar route to the CO. We looked nostalgically at the dumpster and thought, "No, not now, later." Upon arrival, we were forced to wait outside while our guide, the System Manager, was being notified. He finally appeared and greeted us pleasantly. Much to my surprise, he did not look like a standard telco employee, for he did not wear the obligatory flannel shirt. We entered the building and took the elevator to the switching room. I took control of the situation by BS'ing our guide while The Shadow copied down anything he could find written on the walls, etc. We were shown a #1 Crossbar Tandem and the ESS #1A, which were co-residents on the switching floor. We examined the billing tape drives and asked several questions as to the nature of the tape. After 20 minutes or so on the switching floor, he took us to the floor where the wires came in from the outside. While on this floor we also noticed a TSPS machine, of which he had little knowledge, since "that's AT&T." After asking a few more questions and taking more notes, he gave me his number and told us to call him if we had any more questions. We left our friendly tour guide and returned to our car parked conveniently by the dumpster and drove off.

Some Facts

The tour was very informative. We had several misconceptions cleared up. The first and probably most important thing cleared up by the tour was the mystery of the *billing tape*. Exactly what does it contain? The tape contains records of the following types of calls: 0-, 1-, and 2-digit numbers out of your local calling area. In other words they only record the numbers that you or someone else will have to pay for (1-800, collect calls as well). The tapes are then sent to the billing office which handles the billing for both the local Bell and AT&T. According to our guide, the ESS does *not* keep track of every digit dialed. This is not to say that it can't be done, but that it would be impractical. His CO handles well over a million calls a day, and if it were to keep track of all the digits dialed, the storage requirements would be tremendous. Does the ESS print out a list of exceptional 1-800 callers every day? The answer is *no*, the ESS does *not*! But the billing tape does contain records of 1-800 usage, and that type of processing may be done by the billing department, not the CO.

During the tour, we were introduced to the ESS #1A. Our ESS is running a #7 generic program. The #9 generic program is the revision that identifies the number calling you before you answer. It consisted of two equipment racks, each 6'x10', full of printed circuit boards and IC's. All of the boards were push-in, pull-out for easy servicing. One might think from the description of the ESS that we have given that it does not require much space. The ESS processor does not require much space at all, but the equipment that interfaces the local loop with the call processor requires quite a bit more. Unknown to most, the ESS #1A consists of two independent processors that are constantly checking each other. They perform diagnostics if discrepancies do occur. This is a technique similar to

the one used by the space shuttles' computers except that it is more reliable. You cannot shut down the ESS and put a whole town out of touch with the world just because the computers don't agree. The ESS is programmed via magnetic tape drives. The ESS stores the information about its configuration and information about your phone line (special features like call waiting, call forwarding, speed calling, touch or rotary dialing) on two massive hard drives.

Fiber optics are in use! As my group discovered, they are being put on poles all over the place. The cabling is called Light Guide and is made by Western Electric. The transmission system used is called SL C-96 (Slick 96). This system carries 96 simultaneous phone conversations on a single optic fiber. Our guide unfortunately did not know more than the name of the system and its capabilities.

How You Can Meet Your CO

You probably would like to know how you can arrange your own CO tour. You've spent all that time staring in, but now you're willing to meet all those nice people inside. The first thing to do is to find a group to go with. The people at the telco are more likely to let a legit organization visit, rather than just a random group of people. Having just one or two people show up will really make them suspicious. Be sure to take along at least one responsible person to make it look legit. Try groups such as the Boy Scouts, an Explorer Post, a school class, a computer club, or simply come up with a legitimate-sounding name (not the Legion of Doom or the 2600 Club). This group should consist of people who logically have an interest in the phone system - the Audubon Society might seem a little out of the ordinary. The group should be interested in electronics. A bored group will want to move on quickly, despite your interest. Don't take any phreaks, as the telco may get suspicious. The person who attempts to set up the tour should also have no record with Bell Security, as a routine check might be implemented. Be sure to get a good mix of technical, nontechnical people on the tour.

After finding such a group, you should contact the local telephone company's public relations office. Companies are worried about their image, for people tend to acquire an anti-big-business bias when they receive big bills. They will jump at the opportunity to combat this prejudice, and will do their utmost to ensure a tour, even over the objections of workers. Set up a mutually convenient time for your appointment and let your group know.

Proper planning is the best way to maximize information gathering. Questions should be thought out in advance. The questions should start out non-technical, gradually progressing toward the technical as the guide lets down his/her guard. Be careful not to make the questions obviously phreak-oriented. Ask about common knowledge and general interest subjects, such as equal access, the AT&T split-up, fiber optics, and just how does my call get where it is going. Remember, the guide thinks he is showing around another group of idiots. Questions relating to phraud should be asked innocently, and with references that you have heard about this terrible, dreadful subject in the popular media. Questions about blue boxing should quote articles about general phreaking and hacking, *Newsweek* articles, and "\$12,000 calling card bills delivered via UPS" news stories. Remember, you don't want to put him on his guard. For better results, spread your questions around for trustworthy friends to ask. Don't be stingy for you don't want all the attention.

On the actual day of the tour, be sure to bring along notebooks. You will want to record this event for posterity, and for your phriends. If the guide comments on your note taking, just say you are going to write a report for school or an article for your club's newsletter (sounds familiar). Take down any test or other numbers you see on the wall, but try not to "horrow" or you could be in big trouble. We have heard, third hand, of some phreaks on a CO tour who took whatever they could down their shirts, etc. After the tour they were taken into a room where they were forced to disgorge all they had phrond. It isn't worth the risk to steal.

On the tour, conduct yourself properly, as you don't want to stand out. Resist the urge to answer other's stupid questions yourself. Do not show off knowledge. Only gently prod the tour guide on subjects you are interested in. The tour guide will usually give you his number for further questions. Be sure to keep it. Make sure to leave a good impression so that fellow telecommunications hobbyists can tour the place in the future.

These basic techniques can be used to get a tour at almost any location. Other places you might consider are local AT&T Bell Research facilities, GE, Northern Telecom manufacturing plants, or any computer center. On a tour you can easily pick up information that is difficult or impossible to find otherwise. At the very least you can get the type of switch your CO uses. For the most accurate information on your telephone system, go right to the source, your local CO!



The Next Step in Custom Calling

By Tom American Staff Writer

Most Austin (Texas) telephone users who are harassed by obscene or threatening phone calls now have a way to trace those calls. Southwestern Bell is offering a "customer originated trace" service for most Austin customers as part of a test marketing of several advanced custom calling features. The program is called custom calling services plus and Austin is the first city hooked up to it by Southwestern Bell. Phone customers with numbers beginning with 4 or 8—nearly 60 percent of all Austin customers—will have the service available. The following services will be offered:

- **Customer originated call tracing.** Phone users can immediately dial a code to automatically trace harassing phone calls. Upon customer request, Southwestern Bell will notify law enforcement authorities of the traced phone number. Bell, however, will not divulge the identity of the obscene caller to the phone customer. Each tracing of a call will cost \$5.

- **Selective call rejection.** Calls can be routed to a special recording to explain that calls will not be accepted at that time. Customers can also reject subsequent calls from whoever called last. It is not necessary to know the number. The cost is 25 cents to establish a "reject list" and 10 cents a day for maintaining the list.

- **Selective call forwarding.** Incoming calls from three designated numbers can be sent to another remote telephone number. The cost is 10 cents for each time used.

- **Automatic re-call.** A customer can call back the last person who called or the last number the customer called. The cost is 20 cents for each use.

- **Distinctive ringing.** Calls from three designated numbers will ring with a distinctive sound. The cost is 25 cents for each use and 10 cents a day.

"There's no need to sign up for anything," said Bob Dunbar, Austin division manager for Southwestern Bell. "You just pick up the phone and dial the right code for the feature you want to use. It's that simple."

Southwestern Bell will offer the services for one year in Austin to determine if they should be offered systemwide.

"If this service is made available throughout the country, it could be a major deterrent to obscene or threatening calls," Dunbar said. The custom calling system will trace obscene calls only if they originate from a phone in the service area. For more information, give a call to 5124958010.

Industrial Espionage Seminar

By Tom American Staff Writer

Hackers and phone phreaks and what they can do to your computer and your business will be one of the features of the Industrial Espionage and Countermeasures seminar to be held in Florida April 25 and 26, 1985.

The objective of this seminar is to provide the participants with factual information in layman's terms so that they can evaluate their company's vulnerabilities and begin to develop protective systems to guard their data, proprietary information, and communications.

For more info, contact Jim Ross at 3018318400 or write to Russ Engineering Associates, Inc., 7906 Hope Valley Court, Adamstown, MD 21710.

Kenyan Pay Phones Prove Popular

By Tom American Staff Writer

In the first phase of a project to provide affordable telephone service to the masses of Kenya, 3,500 pay phones are being installed throughout this Texas-sized nation.

Judging from the long lines that form at the pay booths, talking—lots of it—is very much in vogue. The scene played out on any day at the row of public phones outside Nairobi's main post office is repeated in the various nooks and crannies of this East African nation.

A caller—coins and personal directory in hand—occupies the booth. Three people patiently wait for their turn. The conversation grows longer; so does the line. Soon there are 6, 7, then 10 people standing in line, all casting querulous glances at the talkative offender. Some Kenyans have taken to calling this affliction "telephonia."

Simon Gachuka was number 8 in line recently outside the post office on the wide thoroughfare of Kenyatta Avenue. Peering over the heads of the long-suffering others, he stared at the booth's occupant and then rolled his eyes in exasperation.

"What is there to talk so long about?" he asked to no one in particular. "What is the romance with the telephone? I came to make a quick call and now the whole lunch hour is spent waiting for the end of a conversation that probably has no known significance."

This Month's Troublemakers

By Tom American Staff Writer

A Marquette (Michigan) man who authorities say devised and used a scheme to evade long-distance telephone fees has been charged with 148 counts of wire fraud. He made 112 calls by dialing 980, a number used by Michigan Bell employees to test equipment, and then "applying multi-frequency tones to the line to call whatever telephone number he wanted," states the indictment. By using the three-digit number, which "was not generally known" about by the company's customers, none of the calls were recorded on the billing computer.

The indictment also alleges that the man [identified to us as Flash Hower, "the



untraceable phreak of the Great White North"] made 28 long-distance calls that were fraudulently charged to Martin Marietta Corp., through the corporation's Wide Area Telephone Service (WATS) line at its Orlando, Florida aerospace division.

The indictment further accuses him of making eight calls that were charged to individual customers of LDX Corp., a St. Louis, Mo., company that sells long-distance phone service.

If convicted, the offender faces a maximum penalty of 740 years imprisonment and a \$740,000 fine.

Associated Press

Three teenagers have been charged with using home computers to make free long-distance telephone calls estimated to be worth hundreds of thousands of dollars or more.

Police spokesmen said the youths, all from northwestern suburbs of Chicago, have been charged with theft of service—a felony—regarding the long-distance calls. They have also been charged with illegal use of a computer, called "hacking"; a misdemeanor.

The teenagers range in age from 14 to 15. They probably will receive probation because none has a criminal record.

The phone companies might seek restitution from the youths' parents.

Newsweek

The parents of "Echo Man," 16, "Three Rocks," 15, and "Uncle Sam," 17, probably thought they were in their rooms doing homework. Instead, the Burlingame, California teenagers were programming their Apples to scan the Sprint telephone-service computers for valid access numbers, which they used to make free calls. They had the numbers on an electronic bulletin board, so others could share in the spoils. That was their undoing. Local police, who had been monitoring the bulletin board, raided each of the hackers' homes and found enough evidence to charge them with felony theft and wire fraud. But the police chose not to prosecute if the youngsters agreed to pay Sprint for the calls and write 10-page papers—on *typewriters*, no less—on the evils of computer hacking.

A Mechanical Hacker

Time

When Clark Dill, director of sanitation for the City of Fayetteville, N.C., came to work one day recently, he found an intriguing little mystery on his hands: despite the fact that his department is locked and deserted each night, switchboard computer records showed that more than 100 telephone calls—most within seconds of each other—had been placed overnight from two telephone extensions.

Burglars? Electronic pranksters? Turns out it wasn't an intruder at all, but two Coca-Cola machines trying to phone home. Both had been equipped with computers to let the local distributor know when it was time for a refill. "The Coke machines were calling the computer at the Coke company and for some reason the computer just wouldn't answer," said Dill. "So the machines just kept calling and calling and calling."

Redemption for a Hacker

By Tom American Staff Writer

A 35-year-old boy who once broke into a bank's computer has eased his conscience by helping the police to crack a computer code that led to evidence sought in a child sex abuse investigation, the authorities say.

It took just 45 minutes to unravel what the police had puzzled over for nearly a month.

A police spokesman said the computerized accounts appear to be confessions of sorts. But he said he did not know whether they would be useful as evidence.

I.R.S. Computers Screw Up

By Tom American Staff Writer

A \$100-million computer system that was supposed to speed the processing of federal income tax returns by the Internal Revenue Service has developed so many glitches that many taxpayers expecting refunds will have to wait about 10 days longer than last year for their checks.

I.R.S. officials said there have been numerous breakdowns of the Sperry Univac 1100-84 computer system since it was installed last fall in the I.R.S.'s 10 regional processing centers. "Anytime you put a new system in, there are going to be problems," said Bob Hughes, director of the I.R.S.'s Holtsville (New York) service center. "They are not catastrophic in nature. But they are irritating as hell."

Hughes said, "I'm convinced we now have a solid system." Moments later, however, he was announcing yet another computer breakdown over the center's public-address system. "A few minutes ago, we lost part of the system—but not the mainframe," he said.

Computel Does Exist

By Tom American Staff Writer

Computel, a new phreaker, hacker and technology oriented newsletter, has not failed according to John Reynolds, a Computel employee. Recently they have been receiving complaints because of not publishing after a massive advertising campaign. Reynolds said that the first issue will soon be available. He blamed a broken printing press for the delay and a shortage of funds for the disconnecting of their toll-free number.

THIS MONTH'S LETTERS

For the 2600 reading list:

The *Catalog of Technical Information*, available from Bell Communications Research is a free source of information re: available technical manuals.

LERG Book. Good, but *!W expensive (wouldn't want all the fore phreaks to get it...). Better to get through trashing.

Animal

Joel, A.E., *A History of Engineering and Science in The Bell System: Switching Technology (1925-1975)*, Bell Laboratories, 1982.

Hansler, Donald H., *Communication System Engineering Handbook*, McGraw Hill Book Company, 1967.

Both were 621.3811 on the Dewey Decimal System. The Bell book mentions that there are other books in the series. The Communications Systems one says it is updated periodically, so it may have a more current edition. The Handbook says it also has "The Lineman's Handbook" by Kurtz in the same series. Both are extremely good and bear looking into. Tons of technical (almost too) data. Much better than these "what's the phone company doing with my call" books littering the kiddie sections of the library. I suppose a college library would be an even better place to look, especially one for a college with a good electrical engineering program.

I also found a great nine page, small print article on blue boxing and phreaking history in the June 1983 *Esquire* on page 376. Originally published in October 1971, it provides an excellent background on the state of phreaking in the sixties, with interviews of "Al Gilbertson," Fraser Lucey, Joe Fingrossi, and Captain Crunch.

The Shadow

Dear 2600:

I have one question about phone companies. When using Sprint to call long distance, how can you tell if the company traces? Does Metrophone trace? What about Allnet?

Also, I dialed a few numbers in Columbus, Ohio. When the other side answered, I received some very strange noises... really strange. Please reply.

Kazematic

Dear 2600:

Exactly what can the LD services do if they catch you using their systems illegally? I have heard they can take your whole system and sell it to pay them back. This sounds a little unusual to me. What if the system isn't yours?

What is the criminal term for phreaking if you are just using the LDS to call up a BBS and not a DoD computer? Is it called theft by wire fraud? Hopefully you can answer these questions.

GR

Laws vary from state to state and also when crossing state lines. If, say, you call a long distance service using a local access number and commit fraud, they can get you on a federal law with the logic that the computer you defrauded is in another state, even though you didn't actually call that other state directly. In most cases, wire fraud is what they hit you with. Some states, like California, are more severe. In Alaska, it is illegal to "divert a machine". With regards to long distance companies, we assume that they ALL trace—we suggest you assume the same. We do know when it's more likely: when using a 959 number, when making lengthy calls on the same code from the same number at the same time of day, when everyone in the world seems to know about it, etc. A good phreak can make traces completely useless by rerouting, being untraceable, and brief when possible. Noises are not really a clue to a trace. These companies have been around long enough to figure out how to do file traces—noises are probably just poor connections or faulty equipment. Keep in mind that it's also a lot easier (and cheaper) for the companies to simply listen in to an illegal call and wait for revealing information to be dropped. We doubt, though, that this would hold up well in court. The companies don't really care WHO you call but they are interested in linking as many people together as possible. They may intimidate the called party into revealing the name of the person who called at a certain time, even though there's not a thing they can do to them if they don't talk (that is a very important fact). If necessary, they can take equipment, if they can prove that it was used to commit fraud—it doesn't matter who it belongs to. And they can find a way to keep it if you can't pay them back for "services rendered". When playing the long distance game, security is a must. The consequences are just too unpleasant.

Dear 2600:

Mike Salerno's article, "Getting in the Back Door," [2600, page 2-2] was well written and informative except for the part on UNIX.

It seems that the author has a basic "feel" for UNIX yet he probably only has had experience on one or two systems.

While UNIX may be "simple" compared to other operating systems such as the TOPS-20, it is far from having "some pretty good security measures." One of the original designers of UNIX, Dennis M. Ritchie, affectionately known to some as the supreme "super user," once said, "... UNIX was not developed with security, in any realistic sense, in mind; this fact alone guarantees a vast number of holes."

Mr. Salerno refers to *commands* such as "who", "sync", "help", and "learn" as accounts. Since UNIX is my favorite operating system, used by many of the Bell operating companies and similar to COSMOS, I have had much experience on over a dozen different systems and I have never encountered the above as accounts. Granted, though, it would not be hard to implement; my point is that it is not standard.

The privileged accounts that are on most UNIX systems are "root", "bin", "sys", and "adm". Others such as "games" and "mup" are also on most systems. The former usually has no password or a simple one and is great for "getting your foot in the front door." The latter uses a special protocol and contains files with passwords and telephone numbers to other UNIX systems! The most powerful account is the "root" account which belongs to the "super user"; it can also be

accessed via the "SU" command as mentioned.

The best part about UNIX is that it is set up so that anyone can view anyone else's files. For example, the lowest user in the UNIX hierarchy can usually type "cat /etc/passwd" and the contents of passwd file is dumped with the passwords encrypted. As mentioned, this is good for looking for accounts without passwords and finding out usernames. Also, the passwords are encrypted using a modified version of the DES encryption algorithm. It is possible, if you know the key [yes, there is a rather simple default (use your imagination) and we all know about defaults...], to use the "crypt" command to decrypt the passwords. Also, there is massive documentation on-line along with the source code for all the commands! Also, UNIX is programmed in C, which is an awesome programming language; knowing C is a prerequisite for any serious UNIX hacker. If you know C and have the right accounts, you can easily modify the system to your liking. Another plus for hackers is that all I/O is treated as files which opens up a Pandora's box of fun for hackers.

There are literally hundreds of holes in UNIX for the hacker. I cannot possibly discuss them all here but I am planning on writing an article, "UNIX for Hackers", in the near (?) future.

Granted, though, UNIX can be semi-secure but most UNIX administrators lack the intelligence to realize this.

BIOC Agent 003

Dear 2600:

What is the telephone number for the NSA?

Mikhail Gorbachev

The National Security Agency, which nobody is supposed to know about, is one of the most secretive organizations in existence. Their main phone number is 301686311 but we've heard that they lurk about in 301677 as well. When calling this number, you can ask for their public relations department or any other for that matter. By the way, for some reason which is completely beyond us, this number resides in an XY step office—one of the most primitive switching centers in existence (see page 1-25). Is this any way for an intelligence agency to operate?

Dear 2600:

MCI, Sprint, etc. must be controlled by MF tones. Any idea how they work? Phreaking opportunities?

HK

In actuality, the majority of alternate carriers aren't controlled by MF tones at all. Many utilize standard touch-tones. What they do is store all of the digits until the last one is entered by the subscriber. Then, the computer finds a line in the city (or area) the subscriber is calling to, gets a dial tone, and sends out the 7 digit LOCAL number. This is how they manage to have lower rates—they get to the city by microwave or satellite, etc., in other words, they avoid AT&T. On occasion, though, the alternate companies' lines in other cities get tied up. When this happens, they use leased lines from AT&T as a backup, which costs them extra and probably accounts for the occasional good connection you may get.

Naturally, if these companies are dialing out on local numbers, it must occasionally be possible for someone to dial INTO those same numbers. What happens then? Sometimes nothing at all. Other times you may actually hear conversations. Anything's possible. One way to find out what a company's local number in a particular city is to dial the ANI number for that city after the local area code. New York City's ANI is 958. (Dial 958 in New York and your phone number is read to you.) On a long distance carrier, you may be able to dial 212958XXXX and have a number read.

Most systems are trained to hang up at the sound of 2600 Hertz. Sometimes, though, it will drop to a dial tone in whatever city you called. Touch tones can be used on the distant dial tone, but most phreaks only make "local" 7 digit calls, since they'll never show up on a bill.

Only one long distance service we know of responds to MF tones and that's ITT. They use a special sequence of these tones in a way that's different from AT&T. We haven't figured it out yet.

Dear 2600:

Re October 1984 article in 2600 on switching centers: AT&T has changed the way it routes calls.

Without telling anyone, AT&T shifted from hierarchical routing to non-hierarchical routing. See paragraph 19, page 8 of a Federal Communications Commission document dated January 25. The FCC document is not specific but apparently AT&T changed the software that controls switching.

[Note to all hackers: Have you noticed anything different about the switching of AT&T calls? Let us know.]

Apparently the FCC approves of the new AT&T routing scheme although Albert Halprin, chief, FCC common carrier bureau, is miffed that he was not told of the plans to change ahead of time. If AT&T had told Halprin, a lawyer, he might have filed a 100 page order to AT&T that was impossible to understand let alone comply with. AT&T executives apparently decided that discretion was the better part of valor. That the system was unlikely to crash if the change was made. That the less Halprin knows about the network the better off everyone will be.

Hunter Alexander

P.S. Implications of non-hierarchical switching: Does it reflect the new power of the microcomputer and the competitors of AT&T? Does it show a new egalitarianism has come to what used to be called the telephone company?

If you want to read up on the old way of switching with five levels of hierarchy, get *Notes on the Network*, AT&T, Network Planning Division, Fundamental Planning Section, 1980. We're happy you found out about that. We'll see if we can figure out what the ramifications will be.

* * *

CORRECTION: Last issue's story on COSMOS was not written by Firemonger but by Fire Monger. We regret the error.

The 2600 Information Bureau

Downloaded from Sherwood Forest II. Soon to be a part of the forthcoming 2600 phone book

202-456-1414	WHITE HOUSE	212-986-1660	STOCK QUOTES	800-525-7623	AM EXPRESS CURR EXCH RT
202-545-6706	PENTAGON	914-997-1277	" "	800-424-2424	AM FED OF TEACHERS
202-343-1100	EPA	516-794-1707	" "	800-525-3056	CATTLEMAN NEWS
714-891-1267	DIAL-A-GEEK	201-623-0150	" "	800-525-3085	CATTLEMAN NEWS
714-897-5511	TIMELY	206-641-2381	VOICE OF CHESTER	800-424-9864	EDISON ENERGY LINE
213-571-6523	SATANIC MESSAGES	(TONE IN 111 FOR DIRECTORY)		800-424-9128	DEPT OF ENERGY NEWSLINE
213-664-7664	DIAL-A-SONG	512-472-9941	SPECIAL RECORDING	800-424-9129	IN SPANISH
405-843-7396	SYNTHACER MUSIC	512-472-9936	" "	800-424-8530	HOUSING URBAN DEVLPMT
213-888-7636	DIAL-A-POEM	512-472-9833	" "	800-424-8807	TRANSPORTATION NEWSLINE
213-765-1000	LIST OF MANY NUMBERS	213-935-1111	WIERD EFFECTS!	800-424-0214	DFC OF EDUCATION NEWS
512-472-4263	WIERD	512-472-4263	WIERD RECORDING	800-424-9090	WHITE HOUSE PRESS DFC
512-472-9941	"INSERT .25"	512-472-2181	" "	800-368-5634	MC1 UPDATE
203-771-3930	PIONEERS	512-472-9936	" "	800-221-4945	WOMEN USA NEWS
213-254-4914	DIAL-A-ATHIEST	512-472-9941	INSERT 25 CENTS RECORDING	800-325-0887	ARTS PROGRAM GUIDE
212-586-0897	DJRTY	212-976-2727	P.D.A.	800-621-8094	AMERICAN MED ASSN
213-840-3971	HORDWITZ	619-485-9988	UNKNOWN	800-368-5744	AFL-CIO NEWS SVC
217-429-9532	DIAL-A-PROSTITUTE	619-748-0002	PHONE CO. TESTING LINES	800-424-8086	NATL EDUCATION ASSN
213-765-2000	JOKES	619-748-0003	" " " "	800-238-5342	NATIONAL COTTON COUNCIL
213-372-6244	JOKES	900-410-6272	SPACE SHUTTLE COMM.	800-424-9820	CITIZENS CHOICE NEWS
202-456-1414	WHITE HOUSE	800-321-3052	UNKNOWN	800-511-5040	N.A.M. NEWSLINE
202-965-2900	WATERGATE	800-321-3048	UNKNOWN	800-252-0112	USC NEWSLINE
011-441-930-4832	QUEEN ELIZABETH	800-321-3049	UNKNOWN	800-368-5667	BUSINESS LINE
916-445-2864	JERRY BROWN	800-321-3074	UNKNOWN	800-368-5814	NATL ASSN OF REALTORS
800-424-9090	RONALD REAGAN'S PRESS	800-631-1147	UNKNOWN	800-368-5693	SENATOR HOWARD BAKER
212-799-5917	ABC NEW YORK FEED LINE	213-331-0437	UNKNOWN	800-368-5833	AM HERITAGE FOUNDATION
800-248-0151	WHITE HOUSE PRESS	800-242-4022	SMOG REPORT LOS ANGELES	800-368-5844	COMM SATELITE CORP
415-843-7439	DIAL-AM-EXCUSE	800-367-4710	SMOG REPORT SAN BERNCO	800-368-5560	COIN UPDATE
800-882-1061	AT T STOCK PRICES	300-622-0858	CALIF MED ASSN	300-221-0226	NBA HOTLINE

How to Use the Dial Telephone

To call a number in your own office:


Let's say the number is 254.

Remove the receiver.

Listen for the dial tone—a steady humming sound.

Place your finger in the opening over the figure "2."



 New York Telephone

Move the dial clockwise until your finger strikes the finger stop.

Remove your finger and allow the dial to turn back. Do not push the dial back.


Dial the figures 5 and 4 in the same way.

When you hear a burr-burr-burr sound, the called telephone is ringing.

If you hear a buzz-buzz-buzz sound, the called telephone is busy. If you hear this "busy" signal hang up the receiver and try the call later.

If you make a mistake in dialing, replace the receiver for a few seconds and begin again.

If you have trouble dialing, replace the receiver for a few seconds, then dial the Operator and she will help you.

DETACH HERE  BEFORE CASHING

TO IMPROVE PUBLIC TELEPHONE SERVICE: Here are some of the things we're doing to improve Public Telephone Service —

- Public Telephone repairmen are patrolling the streets constantly to insure quick repairs.
- We've installed new equipment to alert us when a telephone is out of order.
- We've also added equipment to make Public Telephones more resistant to tampering and vandalism.
- You can help too . . . by calling repair service when you see a Public Telephone out of order. We'll fix it fast. And of course, there's no charge for the call.

2-17

BE SURE YOU DIAL CORRECTLY . . . IF IN DOUBT LOOK UP THE NUMBER

NPA	CN/A Number	Rev.	State (#=Province)	NPA	CN/A Number	Rev.	State (#=Province)	NPA	CN/A Number	Rev.	State (#=Province)
201	201-676-7070		New Jersey	413	617-787-5300		Massachusetts	703	304-580-0255	1/85	Virginia
202	304-343-7016		Washington D. C.	414	608-252-6932		Wisconsin	704	912-784-0440		North Carolina
203	203-789-6815		Connecticut	415	415-543-6374		California	705	416-979-3469		Ontario (#)
204	204-949-0900		Manitoba (#)	416	416-979-0123		Ontario (#)	707	415-543-6374		California
205	205-988-7090		Alabama	417	314-721-6626		Missouri	709	### NONE !!!		Newfoundland (#)
206	206-382-5124		Washington	418	514-394-7440	11/84	Quebec (#)	712	402-580-0255	1/85	Iowa
207	617-787-5300		Maine	419	614-464-0123		Ohio	713	713-861-7194		Texas
208	303-293-8777	10/84	Idaho	501	405-236-6121		Arkansas	714	818-501-7251		California
209	415-543-2861		California	502	502-583-2861		Kentucky	715	608-252-6932		Wisconsin
212	518-471-8111		New York	503	206-382-5124		Oregon	716	518-471-8111		New York
215	818-501-7251		California	504	504-245-5330		Louisiana	717	412-633-5600		Pennsylvania
214	214-464-7400		Texas	505	303-293-8777		New Mexico	718	518-471-8111		New York
215	412-633-5600		Pennsylvania	506	506-648-3041		New Brunswick (#)	801	303-293-8777		Utah
216	614-464-0123	10/84	Ohio	507	402-580-0255	1/85	Minnesota	802	617-787-5300		Vermont
217	217-525-5800		Illinois	509	206-382-5124		Washington	803	912-784-0440		South Carolina
218	402-345-0600	1/85	Minnesota	512	512-828-2501		Texas	804	304-344-6040		Virginia
219	317-265-4834		Indiana	513	614-464-0123		Ohio	805	415-543-2861		California
301	304-343-1401		Maryland	514	514-394-7440	11/84	Quebec (#)	806	512-828-2501		Texas
302	412-633-5600		Delaware	515	402-580-0255	1/85	Iowa	807	416-979-3469		Ontario (#)
303	303-293-8777		Colorado	516	518-471-8111		New York	808	212-344-4336		Hawaii
304	304-344-7935	1/85	West Virginia	517	313-223-8690		Michigan	809	212-344-4336		Caribbean
305	912-784-0440		Florida	518	518-471-8111		New York	812	317-265-4834		Indiana
306	306-347-2878		Saskatchewan (#)	519	416-979-3469		Ontario (#)	813	813-228-7871		Florida
307	303-293-8777	10/84	Wyoming	601	601-961-8139		Mississippi	814	412-633-5600		Pennsylvania
308	402-580-0255		Nebraska	602	303-293-8777		Arizona	815	217-525-5800		Illinois
309	217-525-5800		Illinois	603	617-787-5300		New Hampshire	816	816-275-2782		Missouri
312	312-796-9600		Illinois	604	604-432-2996		British Columbia (#)	817	214-464-7400		Texas
313	313-223-8690		Michigan	605	402-580-0255	1/85	South Dakota	818	818-501-7251		California
314	314-721-6626		Missouri	606	502-583-2861		Kentucky	819	514-287-5151		Quebec (#)
315	518-471-8111		New York	607	518-471-8111		New York	900	201-676-7070		Dial-It service
316	816-275-2782		Kansas	608	608-252-6932		Wisconsin				special area code (SAC)
317	317-265-4834		Indiana	609	201-676-7070		New Jersey	901	615-373-5791		Tennessee
318	504-245-5330		Louisiana	612	402-580-0255	1/85	Minnesota	902	902-421-4110		Nova Scotia (#)
319	402-345-0600		Iowa	613	416-979-3469		Ontario (#)	904	912-784-0440		Florida
401	617-787-5300		Rhode Island	614	614-464-0123		Ohio	906	313-223-8690		Michigan
402	402-580-0255	1/85	Nebraska	615	615-373-5791		Tennessee	907	### NONE !!!		Alaska
403	403-425-2632		Alberta (#)	616	313-223-8690		Michigan	912	912-784-0440		Georgia
404	912-784-0440		Georgia	617	617-787-5300		Massachusetts	913	816-275-2782		Kansas
405	405-236-6121		Oklahoma	618	217-525-5800		Illinois	914	518-471-8111		New York
406	303-293-8777		Montana	619	818-501-7251		California	915	512-828-2501		Texas
408	415-543-6374		California	701	402-580-0255		North Dakota	916	415-543-2861		California
409	713-861-7194		Texas	702	415-543-2861		Nevada	918	405-236-6121		Oklahoma
412	412-633-5600		Pennsylvania					919	912-784-0440		North Carolina

Good as of December 1984. List found and uploaded by Shadow 2600. SOURCE: This list was directly taken from a New Jersey Business Office dumpster, and thus this list is complete, having all North American CN/A Bureaus that exist. NOTE: 809 CN/A is for the Bahamas, Bermuda, Dominican Republic, Jamaica, and Puerto Rico



The Cipher Disk

This simple device has a distinguished history. Ever since its first invention it has been repeatedly re-invented in forms only slightly different from the original. Its story shows that man has sought to put the wheel to use in secret communications wherever possible, even as he also does in mechanics.

As invented in Italy sometime before 1470, it had similar concentric disks with the exception that one contained a "mixed" (scrambled) alphabet. Also, in some of the earlier versions, one of the two alphabets was composed of arbitrary symbols in lieu of conventional characters.

The appeal of the disk lay in the fact that with it, encipherment and decipherment could be performed without carrying bulky or compromising written materials.

The cipher disk came into large-scale use in the United States for the first time in the Civil War. The Federal's Chief Signal Officer patented a version of it, very similar to the original Italian disk, for use in flag signaling. Since his flag stations were within the view of Confederate signalmen as often as not, he prescribed frequent changes of setting.

About a half-century later the U.S. Army adopted a simplified version, very similar to this device, in which one alphabet was "standard" and the other "reverse-standard." Although technically this was a step backward, there were compensating advantages since the regularity of the alphabets tended to reduce error. During the period of the First World War and for several years afterward, the Army issued the disk in this form to units that needed a cipher which could be carried and used easily and which would give a few hours' protection to tactical messages.

In using this device you could leave the two disks in the same setting for an entire message, thus producing the simplest possible cryptogram. Or their setting could be changed with every letter of the message and, if the pattern of the setting-changes were complex enough, you would have an extremely secure cipher.